Derivation of the Rules of Quantum Mechanics from Information-Theoretic Axioms

Daniel I. Fivel [†] October 27, 2010

Abstract

Conventional quantum mechanics with a complex Hilbert space and the Born Rule is derived from five axioms describing properties of probability distributions for the outcome of measurements. Axioms I,II,III are common to quantum mechanics and hidden variable theories. Axiom IV recognizes a phenomenon, first noted by Turing and von Neumann, in which the increase in entropy resulting from a measurement is reduced by a suitable intermediate measurement. This is shown to be impossible for local hidden variable theories. Axiom IV, together with the first three, almost suffice to deduce the conventional rules but allow some exotic, alternatives such as real or quaternionic quantum mechanics. Axiom V recognizes a property of the distribution of outcomes of random measurements on qubits which holds only in the complex Hilbert space model. It is then shown that the five axioms also imply the conventional rules for all dimensions.

1 Introduction

Because the conventional rules of quantum mechanics (CRQM) are abstract and unintuitive, there have been many attempts since their formulation by Dirac and von Neumann to derive them from axioms extracted from the experimental data. The axioms are supposed to isolate the essential ingredients of the data that require the CRQM. Specifically they should answer the following questions: (1) Why must we identify the set S of pure states with a Hilbert space and in particular a Hilbert space over the complex field (\mathbb{C}) rather than the real field (\mathbb{R}) or the quaternions (\mathbb{H})? (2) Why must we calculate probabilities by the Born Rule? (3) What precisely is it that excludes a hidden-variable explanation?

We obtain an important clue to the construction of a satisfactory axiomatic system that addresses these questions when we recall that the celebrated quantum logic approach of Birkhoff and von Neumann [1] gives only a very limited restriction on the model. It endows the system with a projective space structure and hence gives meaning to "dimension" but imposes no restriction at all for dimension N=2 (e.g. qubits or spin $\frac{1}{2}$) and almost none for N=3 (e.g. spin 1). Even for N>3, it only tells us that $\mathcal S$ is a projective space over some sort of skew field $\mathbb F$, which is insufficient to derive the Born Rule by means of Gleason's Theorem [2]. Even if $\mathbb F$ is assumed to be $\mathbb C$, Gleason's theorem only works for N>2.

The fact that the CRQM for qubits is the most difficult to derive suggests an axiomatic strategy based on information theory in which N=2 subspaces play the fundamental role. Reinforcement for this strategy comes from the recognition [3–5] that, even for a system prepared in a pure state, there are different probability distributions for the outcomes of different measurements. When this is taken into account, it was shown in [5] that the appropriate measure of the removal of uncertainty when the outcome of a measurement is known is not the von Neumann entropy, but rather the so-called *information entropy* computed by averaging the Shannon entropy over the outcomes of all possible measurements. Unlike the von Neumann entropy, the

Electronic address: fivel@umd.edu

[†] Department of Physics, University of Maryland College Park, MD 20742

information entropy is *model dependent*, and as the following table shows, can distinguish between real, complex, and quaternionic quantum mechanics in N=2 subspaces.

Pure state entropy for N=2.

The calculations can be found in section 7 below.

We shall exploit these observations to construct a derivation of the CRQM.

2 Preliminary observations

The data consists of a table of the function

$$p(x,y) \equiv x(y) \to [0,1] \tag{2}$$

which gives the attenuation of a beam of particles prepared by a device labeled x after passage through a detecting device labeled y. In optics, for example, x labels the polarizers and y the analyzers. Since the same device may play either role, we use the same set S of labels for each argument. We refer to devices labeled by the elements of S as filters [8]. We refer to a table giving the values of x(y) for S as its p-table.

We confine our discussion to systems which the CRQM describes by a Hilbert space of finite dimension N. With this restriction the CRQM may be stated as follows:

The CRQM: There is a map $z \to \bar{z}$ from S to a complex projective space $\mathbb{C}P^{N-1}$ for some finite N such that

$$x(y) = |\hat{x}^* \cdot \hat{y}|^2 \tag{3}$$

where

$$\hat{z} \equiv \bar{z}/|\bar{z}|.$$

We refer to this map as the Born Rule correspondence (BRC) between S and $\mathbb{C}P^{N-1}$.

Our axioms will be a minimal set of properties of a p-table from which we can deduce the CRQM as stated. Thus our axiomatization is based on the empirical data in contrast to that of Hardy [9] which is based on what he describes as "reasonable axioms which might well have been posited without any particular access to the empirical data".

One immediately observes two kinds of structure in the p-table of a quantum mechanical system: a metrical structure and a statistical structure. What is special about the p-table of a quantum mechanical system is the way these two structures interact.

It will be helpful to have before us the p-table of a very simple system S_o with N=2 which exhibits the properties we will examine in this section. This table is a skeleton of quantum mechanics in which there are just four filters x, x', y, y' corresponding to states of linearly polarized light which the CRQM describes by

$$\hat{x} = (1,0), \quad \hat{x}' = (0,1), \quad \hat{y} = 2^{-1/2}(1,1), \quad \hat{y}' = 2^{-1/2}(1,-1).$$
 (4)

The p-table for S_o is:

The metrical structure is seen in the resemblance between the *p*-table and a road atlas which gives the distances between a set of cities. Our problem is analogous to that of determining the geometry of the earth from such an atlas. Like a road atlas, which has the special value zero on and only on the diagonal, the

p-table has the special value unity on and only on the diagonal. Like an atlas it is also symmetric about the diagonal. These properties of S_o are shared by the p-table of any quantum mechanical system and are expressed by our first axiom:

Axiom I: For every $w, z \in \mathcal{S}$:

$$w(z) = 1$$
 if and only if $w = z$,
 $w(z) = z(w)$. (6)

The conditional probability that a particle in a beam prepared by a u filter will pass a w filter given that it has first passed a v filter is u(v)v(w). In a classical system the result would be the same if v and w were interchanged. It follows from (6) that this is the case for all u if and only if either v(w) = 1 or v(w) = 0. In the former case the two elements are identical.

Definition 2.1. Two elements u, v such that u(v) = 0 are said to be orthogonal and we write $u \perp v$. If u, v are either identical or orthogonal they are said to be "compatible" or "classically related". If they are neither identical nor orthogonal we write $u \not \subset v$.

In S_o observe that $x\mathcal{C}y, x\mathcal{C}y', x'\mathcal{C}y$, and $x'\mathcal{C}y'$ so that S_o cannot be decomposed into the union of two subsets in which the elements of one are classically related to all members of the other.

Definition 2.2. A frame in a subset S^* of S is a maximal set of mutually orthogonal elements.

It follows from (6) that if x(z) = y(z) for all z, then x(y) = 1, and hence x = y. Thus there is a one-one correspondence between the elements x and the functions x(z), and there is a natural metric on S:

$$d(x,y) = \sup_{z \in S} |x(z) - y(z)|.$$
 (7)

Proposition 2.1. The functions $u(\cdot)$ are continuous with respect to the topology defined by the d-metric.

Proof.

$$|u(v) - u(w)| = |v(u) - w(u)| \le \sup_{u \in \mathcal{S}} |v(u) - w(u)| = d(v, w).$$
(8)

Note: Since there is a one-one correspondence $u \leftrightarrow u()$, we shall often use u to mean u() when no confusion will result.

Observe that d(u, v) takes values between zero and unity, the former if and only if u and v are identical and the latter if and only if u and v are orthogonal. Thus the elements of a frame are a maximal set of maximally separated elements in the d-metric.

The following axiom insures that the number of elements in any frame is finite and that S is complete.

Axiom II: S is compact in the d-metric.

Proposition 2.2. The number of elements in any frame is finite.

Proof. A compact metric space is closed and totally bounded [12]. The latter implies that at most a finite number of elements can be separated by any constant amount. \Box

Note: It is this axiom that will restrict us to systems represented in the CRQM by finite dimensional Hilbert spaces. The closure property will play a role later in the discussion.

A frame consisting of the elements $\mathbf{x} = \{x_1, x_2, \dots\}$ will be denoted $F_{\mathbf{x}}$. In S_o there are just two frames $F_{\mathbf{x}} = \{x, x'\}$ and $F_{\mathbf{y}} = \{y, y'\}$.

Definition 2.3. A frame function on S^* is a probability distribution function on every frame in S^* , i.e. a function ζ from S^* to [0,1] such that

$$\sum_{j} \zeta(x_{j}) = 1 \quad \text{for every frame } F_{\mathbf{x}}. \tag{9}$$

Note: We use the term "frame function" for what Gleason [2] calls a non-negative frame function of weight unity.

Axiom III: The function a(x) is a frame function on S for every $a \in S$.

We refer to frame functions formed in this way from the elements of S as pure states.

The elements of a frame are the possible outcomes of some measurement. The physical interpretation of Axiom III is that $a(x_j)$ is the probability of the outcome x_j when the measurement is performed on a system in the state a. In S_o there are four pure states x, x', y, y'.

In view of the symmetry of p, Axiom III also says that for every frame $F_{\mathbf{x}}$ in S we have

$$\sum_{j} x_{j}(a) = 1 \text{ for every element } a \in \mathcal{S}.$$
(10)

A set of functions with this property is said to be a *basis* of S, whence Axiom III is equivalent to the assertion that every frame in S is a basis of S.

We are led to the notion of "subspace" by considering subsets S^* of S for which a given (not necessarily maximal) set of mutually orthogonal elements is a basis. For elements in this subset, the only possible outcomes of a specific measurement will be one of the finite set of elements of the basis.

Definition 2.4. Let $F_{\mathbf{x}}^* \equiv \{x_1, \dots, x_N\}$ be a set of mutually orthogonal elements of S. The subspace S^* of S spanned by $F_{\mathbf{x}}^*$ consists of elements z for which $F_{\mathbf{x}}^*$ is a basis i.e. for which

$$\sum_{j=1}^{N} x_j(z) = 1. (11)$$

Evidently $\{x_1, \dots, x_N\}$ is a maximal orthogonal set in \mathcal{S}^* since no element can be orthogonal to all of them and satisfy (11). Hence $F_{\mathbf{x}}^* \equiv \{x_1, \dots, x_N\}$ is a frame in \mathcal{S}^* .

Proposition 2.3. An element orthogonal to every element of a frame in S^* is orthogonal to every element of S^* .

Proof. If y is orthogonal to a frame $F_x = \{x_1, \cdots, x_N\}$ on \mathcal{S}^* , then $\{y, x_1, \cdots, x_N\}$ is a subset of some maximal set of mutually orthogonal elements of \mathcal{S} . Hence by (10) $\sum_{j=1}^N x_j(z) + y(z) \leq 1$. But the first term is unity for $z \in \mathcal{S}^*$ whence y(z) = 0.

Proposition 2.4. Every frame in S^* has the same number of elements and spans S^* . Moreover, if $\{x_1, x_2, \dots, x_N\}$ and $\{y_1, y_2, \dots, y_N\}$ are two such frames, then

$$\sum_{j=1}^{N} y_j(w) = \sum_{j=1}^{N} x_j(w) \text{ for all } w \in \mathcal{S}$$
(12)

with common value unity if and only if $w \in \mathcal{S}^*$.

Proof. Extend $F_{\mathbf{x}}^*$ to a frame $F_{\mathbf{x}} = \{x_1, x_2, \cdots, x_N, x_{N+1}, \cdots\}$ in \mathcal{S} . By proposition **2.3** the elements $\{x_{N+1}, \cdots\}$ are orthogonal to every element of \mathcal{S}^* and hence to any maximal set $\{y_1, y_2, \cdots\}$ of mutually orthogonal elements of \mathcal{S}^* . If an element z is orthogonal to x_{N+1}, \cdots , then $\sum_{j=1}^N x_j(z) = 1$, so $z \in \mathcal{S}^*$ and hence cannot be orthogonal to $\{y_1, y_2, \cdots\}$ since this is a maximal set of mutually orthogonal elements of \mathcal{S}^* . Hence $\{y_1, y_2, \cdots, x_{N+1}, \cdots\}$ is a maximal set of mutually orthogonal elements of \mathcal{S} , so that for all $w \in \mathcal{S}$ we have

$$\sum_{j} y_{j}(w) + \sum_{j=N+1}^{\infty} x_{j}(w) = 1.$$
(13)

Since $\sum_{j=1}^{N} x_j(w) + \sum_{j=N+1}^{\infty} x_j(w) = 1$ it follows that $\sum_j y_j(w) = \sum_{j=1}^{N} x_j(w)$ with common value unity if and only if $w \in \mathcal{S}^*$. Thus $F_{\mathbf{y}}^* = \{y_1, y_2, \cdots\}$ spans \mathcal{S}^* , and it remains to prove that this set contains N elements. Let $\{x_1, \cdots, x_N\}$ and $\{y_1, \cdots, y_M\}$ be frames on \mathcal{S}^* so that for any $z, w \in \mathcal{S}^*$

$$\sum_{i=1}^{N} x_i(z) = 1 = \sum_{j=1}^{M} y_j(w).$$
(14)

Put $z = y_j$ on the left side and sum on j to obtain M, and put $w = x_i$ on the right side and sum on i to obtain N. The two double sums are equal by the symmetry (6).

Definition 2.5. The number N is referred to as the dimension of the subspace S^* .

Corollary 2.5. For every element x of a two-dimensional subspace, there is a unique element x' to which it is orthogonal.

Proof. If
$$x \perp x'$$
 and $x \perp x''$, then $x(x'') + x'(x'') = 1 \implies x'(x'') = 1$, i.e. $x' = x''$ by (6).

We refer to x and x' as antipodes and indicate the two dimensional space that they span by $\mathcal{P}_{xx'}$.

3 Effect of measurements on states.

The frame function property of the elements $a \in \mathcal{S}$ means that the probability $b_j(a)$ sums to unity for a particle in a beam prepared by an a-filter to pass one of the filters b_1, b_2, \cdots of a frame $F_{\mathbf{b}}$. The fact that b(b) = 1 for any b means that a beam which is unattenuated by a b filter will be unattenuated by a second b filter. Thus a determination of which filter of frame $F_{\mathbf{b}}$ a system in state a passes transforms the probability distribution function a into the probability distribution function a given by:

$$a \to F_{\mathbf{b}}a = \sum_{j} b_{j}(a)b_{j}. \tag{15}$$

We shall refer to this transformation as a *measurement* of a by $F_{\mathbf{b}}$. It is the transformation referred to in quantum mechanics as "collapse of the wave function".

In view of Axiom III, $F_{\mathbf{b}}a$ is a frame function, since if ρ_1, ρ_2, \cdots are frame functions so also is any convex linear combination of them i.e. any function $\zeta = \sum_j \alpha_j \rho_j$ with $0 \le \alpha_j \le 1$ and $\sum_j \alpha_j = 1$. Frame functions such as $F_{\mathbf{b}}a$ that result from measurements are of a special type in that they are composed of *orthogonal* pure states. We refer to these as *mixed states*. The term "state" will be used to refer to either a pure state or a mixed state frame function.

Note: It is important to keep in mind that we cannot assume at this stage that frame functions composed of convex combinations of non-orthogonal pure states can be written as convex combinations of orthogonal pure states — something we know to be a consequence in the CRQM of the diagonalizability of convex combinations of projection operators representing pure states.

The mixed state $\rho = \sum_{i} \alpha_{i} b_{j}$ has the property that it is unchanged by a measurement of $F_{\mathbf{b}}$, i.e.

$$F_{\mathbf{b}}\rho = F_{\mathbf{b}} \sum_{j} \alpha_{j} b_{j} = \sum_{j} \alpha_{j} F_{\mathbf{b}} b_{j} = \sum_{j} \alpha_{j} b_{j} = \rho \tag{16}$$

but will change for other choices of the frame.

The Shannon entropy of a probability distribution (q_1, q_2, \cdots)

$$S[(q_1, q_2, \cdots)] = -\sum_j q_j \ln q_j.$$
 (17)

measures the removal of uncertainty when an outcome is known. As noted above, Stotland et al [5] observed that if we do not know in advance what measurement is going to be made on a state ρ , then to compute

the removal of uncertainty when a measurement is made on it we should take the average of the Shannon entropy of the outcome distributions from all possible meaurements. This average is called the "information entropy" $\overline{S[\rho]}$. In contrast, the von Neumann entropy $H[\rho]$ considers only the distribution of outcomes when the measurement does not change the state, i.e.

$$H[\sum_{j} \alpha_{j} b_{j}] = -\sum_{j} \alpha_{j} \ln \alpha_{j}. \tag{18}$$

Both the von Neumann entropy and the information entropy provide a measure of the purity of a mixed state. Let us compare them for states belonging to the skeletal system S_o given by the p-table (5):

In S_o there are just two frames $F_{\mathbf{x}}$ and $F_{\mathbf{y}}$. We have $F_{\mathbf{x}}x=x$ and $F_{\mathbf{y}}y=y$. There appear to be two mixed states $F_{\mathbf{x}}y=\frac{1}{2}x+\frac{1}{2}x'$ and $F_{\mathbf{y}}x=\frac{1}{2}y+\frac{1}{2}y'$, but these are in fact identical. To see this observe that $\frac{1}{2}x(z)+\frac{1}{2}x'(z)=\frac{1}{2}=\frac{1}{2}(z(x)+z(x'))$ for every z and the same with y replacing x. The von Neumann entropy of the pure states is zero and of the mixed state is $\ln 2$. The information entropy is $\frac{1}{2}\ln 2$ for the pure states and $\ln 2$ for the mixed state.

In S_o we see a rudimentary form of interference i.e. it can happen that two states formed in different ways (in this case the states $F_{\mathbf{x}}y$ and $F_{\mathbf{y}}x$) turn out to be identical. More generally it follows from (12) that if $F_{\mathbf{x}}^*$ and $F_{\mathbf{y}}^*$ are frames in the same N dimensional subspace, then the maximally mixed states in that subspace are identical, i.e.

$$\frac{1}{N} \sum_{j=1}^{N} x_j = \frac{1}{N} \sum_{j=1}^{N} y_j. \tag{19}$$

Although S_o exhibits this indistinguishability of maximally mixed states, it is not a quantum mechanical system. This may be seen by observing that its statistical behavior can be produced by the following hidden variable model: Let ξ be a hidden variable that takes on values on a circle. When ξ is on the right and left halves of the circle, a particle passes filters x, x' respectively, and when ξ is on the upper and lower halves of the circle, it passes y, y' respectively. The conditional probability that ξ be on the right half, given that it is in the upper half is 1/2. Similarly all of the values in the table are predicted correctly.

The S_o model can be generalized to one with sets of 2(R+1) elements $x_1, x_2, \cdots, x_{R+1}$ and $x_1', x_2', \cdots, x_{R+1}'$ such that $x_j(x_k) = \frac{1}{2}$ and $x_j(x_k') = \frac{1}{2}$ for $j \neq k$. Just as S_o which has R=1 is the skeleton (4) of two dimensional quantum mechanics over the real number field, the case R=2 is a skeleton of two-dimensional complex quantum mechanics with x_1, x_2, x_3 corresponding to $(1,0), 2^{-1/2}(1,1), 2^{-1/2}(1,i)$ respectively and x_1', x_2', x_3' corresponding to $(0,1), 2^{-1/2}(1,-1), 2^{-1/2}(1,-i)$ respectively. The case R=4 is a skeleton of quaternionic quantum mechanics with additional elements x_4, x_5 and x_4', x_5' corresponding to $2^{-1/2}(1,\pm j)$ and $2^{-1/2}(1,\pm k)$ where 1,i,j,k are the quaternionic units. None of these skeletons are quantum mechanical since, as for S_o , the function x(y) can be reproduced by a hidden-variable ξ ranging over an R-sphere: If the cartesian coordinates of ξ are $(\xi_1, \cdots, \xi_{R+1})$, a particle passes an x_j or x_j' filter according as ξ_j is positive or negative.

4 The entropic Turing-von Neumann effect

We see then that there is a crucial ingredient of quantum mechanics not accounted for in S_o or any of these generalizations. A clue to the missing ingredient comes from a comparison of the information entropy of a pure state in the three skeletal models with that of real, complex, and quaternionic quantum mechanics given in the following table:

Information entropy for N=2 pure states

skeleton
$$\mathbb{R}$$
 \mathbb{C} \mathbb{H}

$$\frac{1}{2} \ln 2 \quad \frac{2}{3} \ln 2 \quad \frac{4}{5} \ln 2$$

$$qm \quad 2 \ln 2 - 1 \quad 1/2 \quad 7/12$$

$$qm - skeleton \quad 0.040 \quad 0.037 \quad 0.029$$
(20)

We see that the quantum mechanical values are slightly larger than those of the skeletons, which tells us that there have to be more possible measurement frames to account for it. The effect of a measurement described by the frames $F_{\mathbf{x}}$ and $F_{\mathbf{y}}$ in S_o is either to leave a pure state alone or transform it into the maximally mixed state. Thus the von Neumann entropy change is either zero or $\ln 2$ in any measurement. In quantum mechanical systems, however, we observe that the increase in von Neumann entropy resulting from a measurement can be reduced by making a suitable intermediate measurement. This phenomenon, which was first noted by Turing [10] and elaborated by von Neumann [11] is related to the so-called Zeno effect in which the dynamic evolution of a state is arrested by continuous monitoring.

In order for the increase in von Neumann entropy resulting from the measurement of $F_{\mathbf{b}}$ on a to be reduced by some intermediate measurement, there must be a frame $F_{\mathbf{c}}$ such that

$$H(F_{\mathbf{b}}F_{\mathbf{c}}a) < H(F_{\mathbf{b}}a). \tag{21}$$

For $F_{\mathbf{c}}$ to accomplish this, it must transform a into a state which in some sense lies "between" a and b. A natural candidate for such a state is one of the form $\rho = \alpha a + (1 - \alpha)b$ with $0 < \alpha < 1$. Although this is not a combination of orthogonal pure states, we have seen above that it is possible for two frame functions formed in different ways to be identical, and hence some measurement of $F_{\mathbf{c}}$ on a can in principle produce a frame function identical to ρ . The resulting entropy will be smallest if the combination involves just a single pair of orthogonal states c, c'. The following axiom asserts that such a measurement does indeed exist, and, as we shall see, this will produce the entropic Turing-von Neumann effect. It is the key property distinguishing quantum mechanical from classical systems.

Axiom IV: Given any two distinct elements $a, b \in \mathcal{S}$ there exists a pair of orthogonal elements c, c' and a number $0 < \alpha < 1$ such that

$$a(c)c + a(c')c' = \alpha a + (1 - \alpha)b. \tag{22}$$

The following are consequences of Axiom IV and Axiom I:

Proposition 4.1.

$$a(c) + a(c') = 1.$$
 (23)

$$b(c) = a(c), \ b(c') = a(c').$$
 (24)

$$\alpha = \frac{1}{2}.\tag{25}$$

$$a(c) = \frac{1}{2}(1 \pm \sqrt{a(b)}).$$
 (26)

Proof. The left side of (22) is a frame function since the right side is. Hence equation (23) holds. Substitution of z = c in the arguments of the functions c, c', a, b in (22) gives

$$a(c) = \alpha a(c) + (1 - \alpha)b(c), \tag{27}$$

whence a(c) = b(c) since $\alpha \neq 1$. Similarly substitution of z = c' gives a(c') = b(c') proving (24). Substituting z = a and z = b in the arguments and using (23,24) we have

$$a(c)^{2} + (1 - a(c))^{2} = \alpha + (1 - \alpha)b(a), \tag{28}$$

$$a(c)^{2} + (1 - a(c))^{2} = \alpha a(b) + (1 - \alpha,$$

whence, since $a(b) \neq 1$ for $a \neq b$, we obtain (25) and (26).

Since the interchange of c and c' changes a(c) to a(c') = 1 - a(c) we can choose c and c' such that $a(c) \ge \frac{1}{2}$, i.e. assume the solution with the + in (26).

Hence we have:

Equivalent form for Axiom IV

Given $a \neq b$ there exist orthogonal states c, c' and a number λ such that

$$\frac{1}{2}(a+b) = \lambda c + (1-\lambda)c' \quad with \ \frac{1}{2} \le \lambda \le 1.$$
 (29)

It will then follow from the substitutions used above to obtain (23 - 26) that

$$\lambda = a(c) = b(c) = \frac{1}{2}(1 + \sqrt{a(b)}). \tag{30}$$

Note that (29) is a second example of an interference phenomenon in which two frame functions formed in different ways turn out to be identical. What it says is that every mixture of two orthogonal states is indistinguishable from some equal mixture of two states. (Its validity in the CRQM follows from the diagonalizability of density matrices.)

We shall often use the special form taken by (29) when the argument of the functions a, b, c, c' is a member of the subspace $\mathcal{P}_{cc'}$ spanned by c, c' so that c'(z) = 1 - c(z), namely:

$$\frac{1}{2}(a(z) + b(z)) = (2\lambda - 1)c(z) + (1 - \lambda), \quad z \in \mathcal{P}_{cc'}.$$
 (31)

From (23,24) this applies to z = a, b and of course to z = c, c'.

We next derive a number of propositions that follow from Axioms I-IV that will play a role in the subsequent analysis:

Proposition 4.2. If a and b are not orthogonal the solution c, c' of (29) is unique.

Proof. If a, b are not orthogonal, then $\lambda \neq \frac{1}{2}$. If g, g' are also solutions of (29) it follows from (31) with z = g that $(2\lambda - 1)c(g) = (2\lambda - 1)g(g)$ from which c(g) = 1 and hence g = c.

Note: When we wish to emphasize that c, c' and λ in (29) are uniquely determined by a non-orthogonal pair a, b, we will write c = c(a, b), c' = c'(a, b) and $\lambda = \lambda(a, b)$.

Proposition 4.3. A pair of distinct states a, b belong to a unique two dimensional subspace \mathcal{P}_{ab} .

Proof. It follows from (23,24) that a, b belong to $\mathcal{P}_{cc'}$ Suppose a and b belong to another two dimensional subspace $\mathcal{P}_{gg'}$. Add the two equations obtained from (29) by setting z = g and z = g'. Since $a, b \in \mathcal{P}_{gg'}$, the left sides will sum to unity, and we obtain

$$1 = \lambda(c(q) + c'(q)) + (1 - \lambda)(c(q') + c'(q')). \tag{32}$$

Since there is some maximal set of mutually orthogonal elements containing c, c', the coefficients of λ and $(1 - \lambda)$ lie between zero and unity as does λ . Hence the only solution is for both coefficients to be unity. Hence g, g' must lie in the subspace $\mathcal{P}_{cc'}$, and hence by proposition **2.4** the subspaces $\mathcal{P}_{gg'}$ and $\mathcal{P}_{cc'}$ are identical.

Corollary 4.4. Two two-dimensional subspaces are either disjoint, identical, or have just one point in common.

Proposition 4.5. If x is orthogonal to two distinct states a, b, it is orthogonal to every member of \mathcal{P}_{ab} .

Proof. From (29) if $x \perp a$ and $x \perp b$, then $x \perp c$ and $x \perp c'$. Hence by proposition **2.3** x is orthogonal to the subspace spanned by c and c' i.e. it is orthogonal to \mathcal{P}_{ab} .

Definition 4.1. Two elements x, y are said to be "mutually equatorial" if $x(y) = \frac{1}{2}$, and we write $x \smile y$. The set of elements equatorial to a given element z is referred to as the equator opposite z and denoted \mathcal{E}_z .

Proposition 4.6. If $a \mathcal{C}b$ belong to a two-dimensional subspace \mathcal{P} , and $a, b \in \mathcal{E}_z$ for some $z \in \mathcal{P}$, then $c(a, b) \in \mathcal{E}(z)$.

Proof. Solve (31) for c(z) with $a(z) = b(z) = \frac{1}{2}$. Noting that $\lambda \neq \frac{1}{2}$ for $a \not \subset b$, we obtain $c(z) = \frac{1}{2}$.

Proposition 4.7. Let a and b be distinct and non-orthogonal, and let b' be the antipode of b in \mathcal{P}_{ab} . Then

$$c(a,b) \smile c(a,b'). \tag{33}$$

Proof. Since $a(b) \neq 0$ or 1 implies that $a(b') \neq 0$ or 1, it follows from (29) that there exists a unique orthogonal pair e, e' such that

$$\frac{1}{2}(a(z) + b'(z)) = \gamma e(z) + (1 - \gamma)e'(z), \tag{34}$$

where

$$e = c(a, b'), \ e' = c'(a, b'), \ \gamma = \lambda(a, b') = \frac{1}{2}(1 + \sqrt{p(a, b')}).$$
 (35)

Since a and b' belong to $\mathcal{P}_{ee'}$ as well as \mathcal{P}_{ab} , it follows from proposition **4.4** that e, e' belong to \mathcal{P}_{ab} . Thus both e, e' and b, b' span \mathcal{P}_{ab} , whence from proposition **2.4**

$$b(z) + b'(z) = e(z) + e'(z) \quad \text{for all } z \in \mathcal{S}.$$
(36)

Combining this with (34), we obtain

$$a(z) - b(z) = (2\gamma - 1)(e(z) - e'(z)). \tag{37}$$

Since $a(b') \neq 0$, it follows that $\gamma \neq \frac{1}{2}$. Putting z = c(a, b) the left side is zero by (29), whence e(c) = e'(c). But e(c) + e'(c) = 1 since $c \in \mathcal{P}_{ee'}$, whence $e(c) = \frac{1}{2}$.

Since Axiom IV was motivated by the entropic Turing-von Neumann effect we must verify that it does indeed follow from it, i.e. we must show that there is an intermediate measurement that reduces the increase of von Neumann entropy caused by a measurement:

Lemma 4.7.1. Let $\rho = \alpha a + (1 - \alpha)a'$ be a state in the two dimensional subspace \mathcal{P} , and let σ be the maximally mixed state. The von Neumann entropy $H(\rho)$ increases monotonically as the distance $d(\rho, \sigma)$ decreases.

Proof. By (19) $\sigma = \frac{1}{2}a + \frac{1}{2}a'$ so that

$$d(\rho, \sigma) = \sup_{z} |\rho(z) - \sigma(z)| = |\alpha - \frac{1}{2}|\sup_{z} |a(z) - a'(z)| = |\alpha - \frac{1}{2}|.$$
(38)

The assertion follows from the fact that

$$f(\mu) = -(\mu \ln \mu + (1 - \mu) \ln(1 - \mu)) \tag{39}$$

is a monotonically decreasing function of $|\mu - \frac{1}{2}|$ on the interval $0 \le \mu \le 1$.

Proposition 4.8. If $a \neq b$, there is a measurement $F_x^* = \{x, x'\}$ with $x \in \mathcal{P}_{ab}$ such that

$$H(F_b F_x a) < H(F_b a). \tag{40}$$

Proof. Let σ be the maximally mixed state in \mathcal{P}_{ab} . Let c=c(a,b) and e=c(a,b') as defined in the note following Proposition 4.2. If $a(b)\geq \frac{1}{2}$, choose x=c, and if $a(b)<\frac{1}{2}$, choose x=e. We have: $F_ba=\tau b+(1-\tau)b'$ with $\tau=a(b)$, whence $d(F_ba,\sigma)=|\tau-\frac{1}{2}|=|a(b)-\frac{1}{2}|$. On the other hand $F_bF_ca=F_b(\frac{1}{2}(a+b))=\mu b+(1-\mu)b'$ with $\mu=\frac{1}{2}(1+a(b))$, whence $d(F_bF_ca,\sigma)=|\mu-\frac{1}{2}|=a(b)/2$. If $a(b)\geq \frac{1}{2}$, then $a(b)/2>|a(b)-\frac{1}{2}|$, so that $d(F_bF_ca,\sigma)>d(F_ba,\sigma)$, and hence $H(F_bF_ca)<H(F_ba)$ by Lemma 4.7.1. If $a(b)<\frac{1}{2}$, the replacement of F_c by F_e replaces b with b', and since $a(b')>\frac{1}{2}$, the same conclusion is obtained.

Although the metric d(x, y) as defined by (7) seems to require a knowledge of x(z) and y(z) for all z, we shall see as a by-product of (37) that it is determined by x(y) alone, and the form of that dependence is inconsistent with local hidden variables:

Proposition 4.9.

$$d(a,b) = \sqrt{1 - a(b)} \text{ for all } a, b \in \mathcal{S}.$$

$$\tag{41}$$

Proof. We can assume $a(b) \neq 0$ or 1, since otherwise the assertion follows from the definition (7) of d. By proposition **2.5**, b has a unique antipode b' in \mathcal{P}_{ab} . Take the supremum over z of the absolute value on both sides of (37) to obtain:

$$d(a,b) = |2\gamma - 1|d(e,e') = |2\gamma - 1| = \sqrt{a(b')} = \sqrt{1 - a(b)}.$$
(42)

Proposition 4.10. If the property (29) holds for S, its p-table cannot be reproduced by a local hidden variable model unless it is classical i.e. unless p only assumes the values zero and unity.

Proof. It is known [13] (see proof in the Appendix) that the relation between d(a,b) and a(b) in any hidden-variable model differs from (41) in that the right side is 1 - a(b) rather than $\sqrt{1 - a(b)}$. Hence such models are inconsistent with Axiom IV unless a(b) only assumes the values 0 and 1 for all elements, i.e. the system is classical.

Comment 4.1. Without the square root the triangle inequality for d becomes

$$x(z) + z(y) \le 1 + x(y),\tag{43}$$

which is Bell's inequality. It is also shown in the Appendix that the CRQM gives (41). This strongly suggests that property (29) has brought us close to the CRQM.

5 Structure of two dimensional subspaces

We shall now exploit Axioms I-IV to show that two dimensional subspaces are isometric to spheres. It is important to distinguish the dimension N=2 of the subspace from the dimension of the spheres which, as we shall see, is determined by the "rank" of the subspace given by the following:

Definition 5.1. The rank R of a two dimensional subspace is one less than the maximum number of elements in a mutually equatorial set.

Proposition 5.1. If \mathcal{P} is a two dimensional subspace of rank R, there is a one-one correspondence $x \to X$ between the elements x of \mathcal{P} and the points X of a unit R-sphere such that

$$x(y) = \cos^2 \frac{1}{2}XY\tag{44}$$

where XY is the angle subtended at the center of the sphere by the arc joining X and Y.

Proof. We shall need several lemmas:

Define $\theta(x,y)$ by

$$x(y) = \cos^2 \frac{1}{2}(\theta(x, y).$$
 (45)

Definition 5.2. A set of elements x_1, x_2, \dots is said to be **properly mapped** to the points X_1, X_2, \dots of an R-sphere if $\theta(x_i, x_j) = X_i X_j$ for all i, j.

To prove Proposition 5.1 we shall prove that there is a one-one proper mapping of the elements of \mathcal{P} to the points of an R-sphere.

Because we are restricting the elements to a two dimensional subspace, we can use the special form (31) of Axiom IV. Rewriting this in terms of θ defined by (45), it becomes:

$$\cos\theta(a,z) + \cos\theta(b,z) = 2\cos\frac{1}{2}\theta(a,b)\cos\theta(c,z),\tag{46}$$

and

$$\theta(a,c) = \theta(c,b) = \frac{1}{2}\theta(a,b). \tag{47}$$

The geometric significance of (46) and (47) is revealed by the following lemma which applies to an R-sphere for any R.

Lemma 5.1.1. Let A, B, C, Z be points on an R-sphere, with C the midpoint of the arc joining A and B. Then

$$\cos(AZ) + \cos(BZ) = 2\cos(\frac{1}{2}AB)\cos(CZ). \tag{48}$$

Proof. If A, B are antipodes, the right and left sides both vanish. Assume they are not antipodes. Let $\hat{\mathbf{x}}_A, \hat{\mathbf{x}}_B, \hat{\mathbf{x}}_Z$ be unit vectors from the center to the points A, B, Z respectively of a unit R-sphere. The vector $\mathbf{x} = \frac{1}{2}(\hat{\mathbf{x}}_A + \hat{\mathbf{x}}_B)$ connects the center to the midpoint of the chord joining A, B. Its length is

$$|\mathbf{x}| = \sqrt{(1 + \hat{\mathbf{x}}_A \cdot \hat{\mathbf{x}}_B)/2} = \cos(\frac{1}{2}AB)$$

which does not vanish if A and B are not antipodes. Hence $\hat{\mathbf{x}}_C = ((\hat{\mathbf{x}}_A + \hat{\mathbf{x}}_B)/(2\cos(\frac{1}{2}AB))$ is a unit vector from the center to the midpoint C of the great circle arc joining A and B. Hence if CZ is the arc joining C and C we have

$$\cos(CZ) = \hat{\mathbf{x}}_C \cdot \hat{\mathbf{x}}_Z = (\hat{\mathbf{x}}_A \cdot \hat{\mathbf{x}}_Z + \hat{\mathbf{x}}_B \cdot \hat{\mathbf{x}}_Z)/(2\cos(\frac{1}{2}AB)) = (\cos(AZ) + \cos(BZ))/(2\cos(\frac{1}{2}AB))$$

whence (48) follows.

Lemma 5.1.2. Suppose that a subset of the two-dimensional subspace \mathcal{P} consisting of z_1, z_2, \cdots is properly mapped to the set of points Z_1, Z_2, \cdots on the R-sphere S_R . Then the subset consisting of $z_1, z_2, \cdots, z'_1, z'_2, \cdots$, where z'_j is the antipode of z_j on \mathcal{P} , is properly mapped to $Z_1, Z_2, \cdots, Z'_1, Z'_2, \cdots$, where Z'_j and Z_j are antipodes on S_R .

Proof. For any elements x, y of the set $z_1, z_2, \dots, z'_1, z'_2, \dots$, we have

$$x'(y) = 1 - x(y) = \sin^2(\theta(x, y)/2) = \cos^2((\theta(x, y) + \pi)/2) = \cos^2((XY + \pi)/2) = \cos^2(X'Y/2)$$

whence

$$\theta(x', y) = X'Y.$$

We refer to the result of this lemma as antipode adjunction to a properly mapped subset.

Lemma 5.1.3. Suppose that a subset of the two-dimensional subspace \mathcal{P} consisting of $a\mathcal{C}b$ and z_1, z_2, \cdots can be properly mapped to the points $\{A, B, Z_1, Z_2, \cdots\}$ on S_R . Let C be the midpoint of the shorter great circle arc joining A, B, and let c = c(a, b) of (29). Then the mapping $c \to C$ extends the proper mapping to the set $\{a, b, c, z_1, z_2, \cdots\}$.

Proof. Let z be any of the z_i 's. If $\{a, b, z\} \to \{A, B, Z\}$ is a proper mapping, it follows from (31) that

$$\cos(AZ) + \cos(BZ) = 2\cos(\frac{1}{2}AB)\cos(\theta(c,z)). \tag{49}$$

If $a\mathcal{C}b$, then $AB \neq \pi$ so that $\cos(\frac{1}{2}AB) \neq 0$, whence from (31) we have

$$\theta(c, z) = CZ,\tag{50}$$

and from (47),

$$\theta(a,c) = \frac{1}{2}\theta(a,b) = \frac{1}{2}AB = AC, \quad \theta(c,b) = \frac{1}{2}\theta(a,b) = \frac{1}{2}AB = CB. \tag{51}$$

Hence
$$c \to C$$
 extends the proper mapping $\{a,b,z\} \to \{A,B,Z\}$ to $\{c,a,b,z\} \to \{C,A,B,Z\}$.

We call the result of this lemma *midpoint adjunction* to a properly mapped subset.

Lemma 5.1.4. Suppose that a subset K of the two-dimensional subspace P can be properly mapped to a unit R-sphere S_R . If $aCb \in K$, there exists a subset C_{ab} of P containing a and b, referred to as a circular subset, which can be properly mapped to a great circle \tilde{C}_{AB} on S_R in such a way that the union of C_{ab} and K is properly mapped to S_R . If a and b belong to the equator E(z) of some state $z \in P$, then every element $y \in C_{ab}$ also belongs to E(z).

Proof. Let \mathcal{P} be a two-dimensional subspace with elements $a\mathscr{C}b$. As shown in Figure 1: Let a and b be mapped to points A, B of a unit great circle $\tilde{\mathcal{C}}_{AB}$ on an R-sphere separated by an arc $\theta(a,b)$. By definition the set $\{a,b\}$ is properly mapped. By antipode adjunction the set $\{a,b,a',b'\}$ is properly mapped to A,B,A',B'. Let $e_1=c(a,b)$ and $e_2=c(a,b')$ be mapped to the midpoints E_1,E_2 of the arcs joining A,B and A,B' respectively and their antipodes to the points opposite. As noted earlier, e_1 and e_2 are an equatorial pair. By the midpoint adjunction the set $\{a,b,e_1,e_2,a',b',e'_1,e'_2\}$ is now properly mapped to $\tilde{\mathcal{C}}_{AB}$.

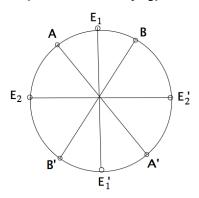


Figure 1

The four points E_1, E_2, E'_1, E'_2 are at points that are equally spaced by $\pi/2$. We can apply midpoint adjunction k times to extend the proper mapping to include elements of \mathcal{P} whose images are spaced by $\pi/2^k$. With k arbitrarily large the images become dense on $\tilde{\mathcal{C}}_{AB}$ in the round-metric. The completion of this set of elements in the d-metric is the subset \mathcal{C}_{ab} of \mathcal{P} . From proposition 4.6 if $a\mathcal{C}b \in \mathcal{E}(z)$, then e_1, e_2 and all successive elements of \mathcal{C}_{ab} obtained by midpoint adjunction will be in $\mathcal{E}(z)$.

Note: Here we used Axiom II to insure the completeness of \mathcal{P} in the d-metric.

Corollary 5.2. If $x \in C_{ab}$ there is a unique pair of states $y, y' \in C_{ab}$ such that $x \smile y$ and $x \smile y'$.

Proof. The required states $\{y, y'\}$ are the points of C_{ab} with images $\{Y, Y'\}$ at the end points of the diameter of \tilde{C}_{AB} at right angles to the diameter joining the images $\{X, X'\}$ of $\{x, x'\}$.

We now combine the results of the above lemmas to complete the proof of proposition 5.1:

Let \mathcal{P} be of rank R so that there are n = R + 1 elements in a maximal set of mutually equatorial elements. Let e_1, e_2, \dots, e_n of \mathcal{P} be any such set. It can be properly mapped to an to a unit R sphere S_R by placing the images E_j of e_j for $j = 1, \dots, n$ at the points of S_R with *i*'th cartesian coordinate δ_{ij} . By Lemma **5.1.4** the proper mapping can be extended to include a subset \mathcal{P}^* of \mathcal{P} with the property that it contains \mathcal{C}_{xy} for every pair $x\mathcal{C}y$ of its elements. We shall prove that $\mathcal{P}^* = \mathcal{P}$ and that the set of images of \mathcal{P} covers S_R .

Suppose first that there is some $x \in \mathcal{P}$ such that $x \notin \mathcal{P}^*$. Then the circular set \mathcal{C}_{e_1x} can contain no point other than e_1 of \mathcal{P}^* for otherwise x would be in \mathcal{P}^* . Hence, by the Corollary to Lemma **5.1.4**, there is an element $f_1 \notin \mathcal{P}^*$ but $f_1 \in \mathcal{C}_{e_1x}$ such that $f_1 \smile e_1$. Now the circular set $\mathcal{C}_{e_2f_1}$ may contain no element of \mathcal{P}^* other than e_2 for otherwise f_1 would belong to \mathcal{P}^* . Since $f_1 \smile e_1$ and $e_2 \smile e_1$ it follows from Lemma **5.1.4** that every element f of $\mathcal{C}_{e_2f_1}$ satisfies $f \smile e_1$. In particular this is true of an element f_2 of $\mathcal{C}_{e_2f_1}$, which exists by the last part of Lemma **5.1.4**, that satisfies $f_2 \smile e_2$. Thus e_1, e_2, f_2 is a mutually equatorial set in which f_2 is not an element of \mathcal{P}^* since otherwise f_1 would be a member. Next we construct $\mathcal{C}_{e_3f_2}$ and repeat this process until we produce a state f_n which belongs to \mathcal{P} but does not belong to \mathcal{P}^* and has the property that $e_1, e_2, \cdots, e_n, f_n$ is a mutually equatorial set. But this makes the rank of \mathcal{P} larger than R which is a contradiction. This proves that $\mathcal{P} = \mathcal{P}^*$.

Proof that S_R is completely covered by the mapping is obtained by essentially the same argument: Suppose that some point X on the sphere does not appear. Then no point Y other than E_1 on the great circle C_{E_1X} can appear. For if Y were the image of some $y \in \mathcal{P}$, then the entire circle would appear as the image of the circular set C_{e_1y} . In particular there is a point F_1 on C_{E_1X} which is equatorial to F_1 and does not occur in the mapping. Similarly no point on $C_{E_2F_1}$ can occur, and every point on it is equatorial to F_1 . In particular

it contains a point F_2 which is equatorial to both E_1 and E_2 . Proceeding in this way we construct a point F_n on S_R which is equatorial to E_1, \dots, E_n which is impossible.

With this result we have established that there is a one-one proper mapping of the completion of \mathcal{P} of rank R to the points of an R-sphere which proves proposition 5.1.

6 Two dimensional subspaces of rank R=2

We next make the connection between two dimensional subspaces with rank R=2 and the CRQM for N=2 subspaces.

Proposition 6.1. There is a one-one correspondence between the points x of a two dimensional subspace of S of rank R=2 and the points \bar{x} of CP^1 such that

$$x_1(x_2) = |\hat{x}_1^* \cdot \hat{x}_2|^2 \text{ where } \hat{x} = \bar{x}/|x|$$
 (52)

which is the Born Rule.

Proof. The space $\mathbb{C}P^1$ is the linear space over the complex numbers with elements represented by two homogeneous coordinates i.e. pairs $\bar{x} = \{\alpha_1, \alpha_2, \}$, not both of which are zero, such that two pairs are identified if their elements differ by a common non-zero complex factor.

There is a one-one correspondence $X \leftrightarrow \bar{x}$ between the points of a unit 2-sphere and the points of $\mathbb{C}P^1$ obtained by stereographic projection, i.e. the correspondence $X(\theta,\phi) \leftrightarrow \hat{x} = \bar{x}/|x|$ between a point on a unit 2-sphere with zenith θ and azimuth ϕ and the point of $\mathbb{C}P^1$ defined by

$$\hat{x} = \left(\cos\frac{1}{2}\theta, e^{i\phi}\sin\frac{1}{2}\theta\right). \tag{53}$$

Let \hat{x}_1 and \hat{x}_2 correspond to $X_1 = X(\theta_1, \phi_1)$ and $X_2 = X(\theta_2, \phi_2)$, and let ξ_1 and ξ_2 be the cartesian components of unit vectors from the center to X_1 and X_2 respectively. Then

$$|\hat{x}_1^* \cdot \hat{x}_2|^2 = \frac{1}{2}(1 + \xi_1 \cdot \xi_2) = \cos^2(\frac{1}{2}X_1 X_2), \tag{54}$$

where X_1X_2 is the great circle arc between points X_1 and X_2 .

The assertion then follows from (44).

Comment 6.1. A similar result is obtained for ranks R = 1 and R = 4. In the former case one maps the 1-sphere to the real projective line $\mathbb{R}P^1$, and in the latter one maps the 4-sphere to the quaternionic projective line $\mathbb{H}P^1$.

7 Picking rank R=2

To complete our axiomatic system we must choose a property of two dimensional quantum mechanical systems which holds only for rank R = 2. One such property pointed out in [15] is that the group of transformations leaving a basis fixed is a continuous, abelian group. However, since our focus in this paper is on information theory, we shall take a different approach based on a property noticed by Sykora [3] and Wootters [4]:

Let x be a state at the north pole of the R-sphere. A measurement in the frame $F_{\mathbf{y}} = \{y, y'\}$ transforms x into the mixture $\rho = py + (1-p)y'$ with $p = \cos^2 \frac{1}{2}\theta$ where θ is the co-latitude of y. We obtain all possible frames by letting y vary over the upper hemisphere. A simple measure of the purity of ρ is $\delta = |2p-1| = \cos \theta$ which is twice its distance from the maximally mixed state in the d-metric and ranges between 0 for the maximally mixed state and 1 for a pure state. The average of any function of the purity $g(\delta)$ (such as the Shannon entropy) over all frames will be given by

$$\overline{g} = \frac{\int_0^{\pi/2} g(\cos\theta)(\sin\theta)^{R-1} d\theta}{\int_0^{\pi/2} (\sin\theta)^{R-1} d\theta} = \frac{\int_0^1 g(\delta)(1-\delta^2)^{(R-2)/2} d\delta}{\int_0^1 (1-\delta^2)^{(R-2)/2} d\delta}.$$
 (55)

For R=2 the right side reduces to $\int_0^1 g(\delta)d\delta$. This is quite remarkable, for what it says is that for R=2 and only for R=2 the purity δ is uniformly distributed on the interval [0,1]. For R=1 the negative power of $(1-\delta^2)$ means that the distribution is weighted towards the pure state value $\delta=1$ whereas for R>2 the positive power of $(1-\delta^2)$ means that it is weighted towards the maximally mixed state $\delta=0$.

This suggests the following choice for our last axiom which picks out R=2:

Axiom V: The purities of the mixed states resulting from random measurements of a pure qubit state are uniformly distributed.

As noted above, the appropriate measure of the removal of uncertainty when a measurement is made is the information entropy which takes account of the lack of pre-knowledge of what measurement is going to be made and requires that we average the Shannon entropy over all possible measurements. The effect of the weighting described above in the real case (R=1) and quaternion case (R=4) is that the information entropy will be smaller than in the complex case for real quantum mechanics and larger for quaternionic quantum mechanics. We verify this by letting $g(\delta)$ be the Shannon entropy

$$g(\delta) = -\left(\frac{1}{2} + \delta\right) \ln\left(\frac{1}{2} + \delta\right) - \left(\frac{1}{2} - \delta\right) \ln\left(\frac{1}{2} - \delta\right) \tag{56}$$

and obtain the values $2 \ln 2 - 1 < 1/2 < 7/12$ for R = 1, 2, 4 respectively.

Given this result we might have considered replacing Axiom V by elevating to axiomatic status the assertion that the information entropy is 1/2 for a pure qubit state. While this "works" to pick out R=2, the fact that the value is 1/2 depends on the choice of the e-base of logarithms in defining the entropy and has no instrinsic physical significance. † In fact one could just as well have chosen the average of any function of the purity δ that differs for different values of R. Axiom V as stated avoids this .

Comment 7.1. The property of a two dimensional complex Hilbert space expressed by Axiom V is a special case of a property of all finite dimensional complex Hilbert spaces proved by Sykora in the appendix to [3], namely that if $F_{\mathbf{y}}x = \sum_{j=1}^{N} p_j y_j$ denotes a mixed state resulting from a random measurement of a pure state x in a complex Hilbert space of dimension N, then $p = \{p_1, \dots, p_N\}$ is uniformly distributed on the "probability simplex" $\sum_{j=1}^{N} p_j = 1$. Sykora further remarks that a different result is obtained for a real Hilbert space. Since we shall deduce the CMQM for N > 2 below from the N = 2 case, we only needed the fact that Axioms I-IV implied the R-sphere structure for N = 2 where the points of the probability simplex are linearly related to the purity δ . Thus we could easily deduce the formula (55) and from it see the uniqueness of the complex case in producing a uniform distribution.

8 Extension to N > 2

It has now been shown that Axioms I-V imply that the qbit subspaces of \mathcal{S} are $\mathbb{C}P^1$ spaces in which the Born Rule holds. In this section it will be shown that this extends to all of \mathcal{S} to produce the CRQM.

To carry this out we must show that the $\mathbb{C}P^1$ coordinatization established for qbits enables us to establish a $\mathbb{C}P^{N-1}$ coordinatization for N dimensional spaces consistent with the Born Rule. To accomplish this we first show that Axioms I-V imply that \mathcal{S} is a projective geometry. While it is intuitively clear that if the two dimensional subspaces of an N-dimensional projective space are $\mathbb{C}P^1$ spaces the space itself must be a $\mathbb{C}P^{N-1}$ space, it is not obvious that a single coordinatization of the space can be carried out in such a way that the Born Rule holds simultaneously in every two dimensional subspace. This will be verified by first showing that there is a coordinatization such that $x(y) = |\hat{x}^* \cdot \hat{y}|^2$ when at least one of the two elements x, y lies on an axis and then showing that it extends to arbitrary pairs.

[†] I am indebted to W. Wootters for this observation.

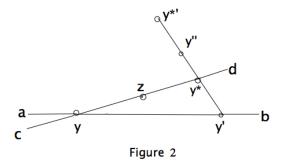
Lemma 8.0.1. S is a projective geometry in which the elements are points, the two-dimensional subspaces are lines, and the three dimensional subspaces are planes.

Proof. We must show that:

(I) Each pair of distinct points are on exactly one line; (II) The Veblen-Young axiom holds (see statement below).

By proposition 4.3 two distinct points a, b determine exactly one two-dimensional subspace \mathcal{P}_{ab} . We must therefore prove (II) which states that if a, b, c, d are four points no three of which are colinear, and if the lines \mathcal{P}_{ab} and \mathcal{P}_{cd} intersect, then the lines \mathcal{P}_{ac} and \mathcal{P}_{bd} intersect. This is an efficient way of asserting that every pair of lines in the plane determined by a pair of intersecting lines will intersect.

We first prove that if \mathcal{P}_{ab} and \mathcal{P}_{cd} intersect they lie in a three-dimensional subspace:



Refer to Figure 2. Let \mathcal{P}_{ab} and \mathcal{P}_{cd} intersect at y. Let y' be its antipode in \mathcal{P}_{ab} , and let y^* be its antipode in \mathcal{P}_{cd} . Let y'' be the antipode of y' in $\mathcal{P}_{y'y^*}$ and let $y^{*'}$ be the antipode of y^* in $\mathcal{P}_{y'y^*}$ Since $y \perp y'$ and $y \perp y^*$ it follows from proposition 2.3 that y is orthogonal to both y'' and $y^{*'}$. Hence both $\{y,y',y''\}$ and $\{y,y^*,y^{*'}\}$ are orthogonal sets. Now let z be any point on \mathcal{P}_{cd} . We have $p(y,z)+p(y^*,z)=1$ whence $p(y^{*'},z)=0$. But since both $\{y',y''\}$ and $\{y^*,y^{*'}\}$ are bases of $\mathcal{P}_{y'y^*}$ it follows from proposition 2.4 that $p(y',z)+p(y'',z)=p(y^*,z)+p(y^{*'},z)=p(y^*,z)+p(y^{*'},z)=p(y^*,z)+p(y^{*'},z)=p(y^*,z)+p(y^{*'},z)=1$. Hence z belongs to the three dimensional subspace spanned by $\{y,y',y''\}$. Since any point on \mathcal{P}_{ab} also lies in this space the assertion follows.

Since \mathcal{P}_{ab} and \mathcal{P}_{cd} lie in a three-dimensional subspace, the lines \mathcal{P}_{ac} and \mathcal{P}_{bd} lie in that subspace, and we can therefore complete the proof of the Veblen-Young axiom by showing that any two distinct lines in a three dimensional subspace intersect.

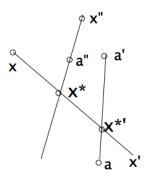


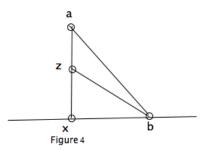
Figure 3

See Figure 3. With no loss in generality we can label the lines $\mathcal{P}_{aa'}$ and $\mathcal{P}_{xx'}$. Since N=3 there are unique elements a'' and x'' such that a, a', a'' and x, x', x'' are bases of \mathcal{S} . The line $\mathcal{P}_{x''a''}$ contains an element x^* which is orthogonal to x'' and hence lies in $\mathcal{P}_{xx'}$. Its antipode $x^{*'}$ is orthogonal to both x^* and x'' and hence is orthogonal to $\mathcal{P}_{x^*x''}$ which is identical to $\mathcal{P}_{x''a''}$. Hence it is orthogonal to a'' so that a'' lies in a'' as well as in a'' and a'' are the velocity and a'' are the proof.

Definition 8.1. Two lines in a plane S^* of S are said to be normal if the antipode of the intersection in one line is orthogonal to its antipode in the other.

Lemma 8.0.2. Let $z \in \mathcal{P}$ and $b \in \mathcal{Q}$ where \mathcal{P} and \mathcal{Q} are normal lines with intersection x. Then b(z) has a maximum at b = x.

Proof. See Figure 4



Recall equation (46)

$$\cos \theta(a, z) + \cos \theta(b, z) = 2\cos \frac{1}{2}\theta(a, b)\cos \theta(c, z),$$

which was derived from (31) under the assumption $z \in \mathcal{P}_{ab}$ which is spanned by c, c' so that c(z) + c'(z) = 1. Here, however, z is only in \mathcal{P}_{ab} when b = x, but since for arbitrary z we have $c(z) + c'(z) \le 1$ we can replace the equation by the inequality:

$$\cos \theta(a, z) + \cos \theta(z, b) \le 2 \cos \frac{1}{2} \theta(a, b) \cos \theta(c, z) \tag{57}$$

with equality if and only if $z \in \mathcal{P}_{ab}$. Since \mathcal{P} and \mathcal{Q} are normal, a is orthogonal both to x and to the antipode of x on \mathcal{P} (not shown in the figure) and hence by proposition **2.3** is orthogonal to every point of \mathcal{P} . Hence $\theta(a,b) = \pi$ so that the right side of (57) is zero. Let $\theta(a,z) + \theta(z,b) = \pi - \epsilon$ so that (57) becomes

$$\cos \theta(a, z) < \cos(\theta(a, z) + \epsilon) \tag{58}$$

with equality if and only if $z \in \mathcal{P}_{ab}$ which occurs for b = x, i.e. $\epsilon = 0$. For small, non-zero $|\epsilon|$ equation (58) implies $\epsilon < 0$, so that $\theta(a, z) + \theta(z, b) \ge \pi$. Hence $\theta(z, b)$ has a minimum at b = x and hence $b(z) = \cos^2 \frac{1}{2}\theta(b, z)$ has a maximum.

Lemma 8.0.3. Let c be the intersection of a pair of normal lines \mathcal{P} and \mathcal{Q} in a plane \mathcal{S}^* . If $a \in \mathcal{P}$ and $z \in \mathcal{Q}$, then

$$a(z) = a(c)c(z). (59)$$

Proof.

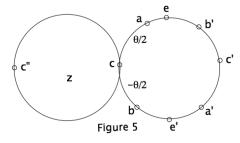


Figure 5 shows a pair of two dimensional subspaces \mathcal{P} and \mathcal{Q} with intersection c that are normal to one another. More precisely it shows the images of these subspaces under the BRC mapping to unit 2-spheres. The antipodes of c on \mathcal{P} and \mathcal{Q} are c' and c'' respectively. z is an arbitrary point of \mathcal{Q} . Since c' is orthogonal both to c and c'' it follows from proposition 4.5 that c'(z) = 0. Hence (29) becomes

$$a(z) + b(z) = 2\lambda c(z)$$
 where $\lambda = a(c) = \cos^2 \frac{1}{4}\theta$. (60)

where θ is the angle between the images of a and b which lie on a great circle through c. By varying the angle θ we can vary a and b on the circle while holding fixed both the midpoint c of a and b and the midpoint e of a and b'. Thus (37) can be written

$$a(z) - b(z) = (2\gamma - 1)K(z)$$
, where $\gamma = \frac{1}{2}(1 + \sqrt{a(b')}) = \frac{1}{2}(1 + \sin\frac{1}{2}\theta)$, (61)

and

$$K(z) = e(z) - e'(z)$$

is independent of θ . Adding (60) and (61):

$$a(z) = \frac{1}{2}K(z)\sin\frac{1}{2}\theta + c(z)\cos^{2}\frac{1}{4}\theta.$$
 (62)

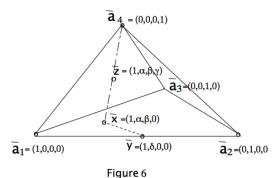
By Lemma 8.0.2 a(z) has a maximum when a is at the intersection point, i.e. at $\theta = 0$. It follows that K(z) = 0 and hence that a(z) = b(z) whence from (60) and (30) we have

$$a(z) = a(c)c(z). (63)$$

Definition 8.2. Let S have dimension N, and let $\mathbf{a} = \{a_1, \dots, a_N\}$ be a basis. The lines $q_{ij} \equiv \mathcal{P}_{a_i a_j}$ with $i \neq j$ are referred to as the axes of the \mathbf{a} -basis. The set $\Omega(\mathbf{a})$ is the set of points belonging to all of the axes of the \mathbf{a} -basis.

Lemma 8.0.4. Let S have dimension N, and let $\mathbf{a} = \{a_1, \dots, a_N\}$ be a basis. Let \overline{S} be a $\mathbb{C}P^{N-1}$ space the elements of which are represented by N component homogeneous complex coordinate vectors $\overline{\xi} = (\xi_1, \xi_2, \dots, \xi_N)$. There is a mapping $z \to \overline{z}$ of the elements of S to \overline{S} such that the Born Rule holds between pairs z_1, z_2 provided that at least one member belongs to $\Omega(\mathbf{a})$.

Proof. By induction: The case N=2 is Proposition 6.1. Assume true for N-1. Map the basis elements a_j to $\overline{a_j}$ with j'th component 1 and the others 0. For $j=1,\cdots,N$ map the N-1 dimensional subspace $\mathcal{S}^{(j)}$ of \mathcal{S} which is orthogonal to a_j to the N-1 dimensional subspace $\overline{\mathcal{S}^{(j)}}$ of $\overline{\mathcal{S}}$ orthogonal to $\overline{a_j}$. By hypothesis of the induction these correspondences can be made in such a way that the Born Rule holds between elements provided at least one of them belongs to one of the axes of $\overline{\mathcal{S}^{(j)}}$. For each $x \in \mathcal{S}^{(j)}$ we map the line $\mathcal{P}_{a_j x}$ to the two dimensional subspace of $\overline{\mathcal{S}}$ spanned by \overline{x} and $\overline{a_j}$ which we can do in such a way that the Born Rule holds between its elements.



To simplify the next part of the proof let us consider the case N=4 (see Figure 6) which will make the general argument clear. The points of $\mathcal{S}^{(4)}$ are mapped to $\overline{\mathcal{S}^{(4)}}$ and so have coordinates of the form $x=(1,\alpha,\beta,0)$. (Note that with homogeneous coordinates we can represent the elements in this way. For example $\alpha\to\infty$ corresponds to the element (0,1,0,0).) If z lies on \mathcal{P}_{a_4x} it will be mapped to a linear combination of x and a_4 and hence to a point $\bar{z}=(1,\alpha,\beta,\gamma)$ for some $\gamma\in\mathbb{C}$. Now let y be an element lying on one of the axes of $\mathcal{S}^{(4)}$ say $\mathcal{P}_{a_1a_2}$ which is mapped to $\bar{y}=(1,\delta,0,0)$ for some $\delta\in\mathbb{C}$. By these mappings the Born Rule holds for the pair z,x and for the pair x,y. Moreover the lines \mathcal{P}_{a_4x} and \mathcal{P}_{xy} are normal to one another since the antipode of x in \mathcal{P}_{xy} lies in $\mathcal{S}^{(4)}$ and hence is orthogonal to the antipode a_4 of x in \mathcal{P}_{a_4x} . Hence by lemma 8.0.3

$$z(y) = z(x)x(y) = |\hat{z}^* \cdot \hat{x}|^2 |\hat{x}^* \cdot \hat{y}|^2 = \frac{|1 + \alpha^* \delta|^2}{(1 + |\alpha|^2 + |\beta|^2 + |\gamma|^2)(1 + |\delta|^2)} = |\hat{z}^* \cdot \hat{y}|^2.$$
 (64)

In similar fashion one establishes that the Born Rule holds between every $z \in \mathcal{S}$ and any element lying on one of the axes of \mathcal{S} .

We are now equipped to prove our main theorem:

Theorem

Axioms I-V imply that there is a mapping of the elements of S of dimension N to a $\mathbb{C}P^{N-1}$ space such that the Born Rule holds between every pair of elements.

Proof. Choose a basis a_1, \dots, a_N of S and perform the mapping described in **Lemma 8.0.4**. Let b_1, \dots, b_N be another basis of S. We have

$$\sum_{j=1}^{N} b_j(s) = 1 \text{ for all } s \in \mathcal{S}^*.$$

$$(65)$$

If s lies on any of the axes $\mathcal{P}_{a_k a_n}$ used for the map above the Born Rule holds between s and every element and in particular between s and b_1, \dots, b_N . Hence:

$$\sum_{j=1}^{N} |\hat{b_j}^* \cdot \hat{s}|^2 = 1. \tag{66}$$

Apply this result when $s = a_k$ for $k = 1, \dots, N$ to obtain

$$\sum_{j=1}^{N} |\hat{b_j}^* \cdot \hat{a_k}|^2 = 1 \text{ for } k = 1, \dots, N.$$
(67)

Also apply it when s is an arbitrary point on the axis $\mathcal{P}_{a_k a_n}$ for all pairs k, n with $k \neq n$ i.e. for $\hat{s} = \alpha \hat{a}_k + \beta \hat{a}_n$ where α and β are arbitrary. For k = n we have

$$\sum_{j=1}^{N} |\hat{b}_{j}^{*} \cdot \hat{a}_{k}|^{2} = 1, \tag{68}$$

and for $k \neq n$

$$(|\alpha|^2 + |\beta|^2)^{-1} \sum_{j=1}^{N} |\hat{b}_j^* \cdot (\alpha \hat{a}_k + \beta \hat{a}_n)|^2 = 1$$
(69)

The second equation works out to

$$\frac{|\alpha|^2}{|\alpha|^2 + |\beta|^2} \sum_{j=1}^N |\hat{b}_j^* \cdot \hat{a}_k|^2 + \frac{|\beta|^2}{|\alpha|^2 + |\beta|^2} \sum_{j=1}^N |\hat{b}_j^* \cdot \hat{a}_n|^2 +$$
(70)

$$2\Re \frac{\alpha^* \beta}{|\alpha|^2 + |\beta|^2} \sum_{j=1}^N (\hat{a}_k^* \cdot \hat{b}_j)(\hat{a}_n \cdot \hat{b}_j^*) = 1$$
 (71)

and since α and β are arbitrary the sum must vanish for $k \neq n$. Hence

$$\sum_{j=1}^{N} (\hat{a}_{k}^{*} \cdot \hat{b}_{j})(\hat{a}_{n} \cdot \hat{b}_{j}^{*}) = \delta_{kn}$$
(72)

Thus the matrix $M_{kj} = \hat{a}_k^* \cdot \hat{b}_j$ is unitary. Hence the coordinates are transformed by a unitary transformation under a change of basis. Given any pair of elements we can choose a basis such that they lie on an axis and hence such that the Born Rule holds between them. But the scalar product is invariant under unitary transformations whence it follows that the Born Rule remains valid in every basis.

We have now completed proof that Axioms I-V imply the CRQM. In the usual Dirac notation we have established that pure states x in S obeying these axioms correspond to kets $|x\rangle$ such that the Born Rule $x(y) = |\langle x|y\rangle|^2$ holds.

9 Discussion

While our derivation of the CRQM from Axioms I-V has been lengthy, we have obtained the result with no dimensional restriction and without having to use Gleason's Theorem which is itself quite lengthy. Moreover our inductive proof of the extension to N > 2 has gotten the result with no more than the rudiments of projective geometry, in particular avoiding the proof that if the planes of an N-dimensional projective space are $\mathbb{C}P^2$ the space is $\mathbb{C}P^{N-1}$ [14].

A key role in the axiomatic system presented here was played by Axiom IV, motivated by the entropic Turing-von Neumann effect in which the loss of purity of a state resulting from a measurement is reduced by an intermediate measurement. It is remarkable that the impurity can be made arbitrarily small by a sufficiently large number of intermediate measurements. Indeed, one can reproduce unitary (Schrödinger) dynamics with arbitrarily high accuracy in this way. For consider a sequence of measurements performed on a system in frames containing states $|n\rangle$ which are related by $|n\rangle = e^{-i\tau H}|n-1\rangle$ for some Hamiltonian H and time interval τ . The probability p_n for finding the system in state $|n\rangle$ after n measurements starting with $|0\rangle$ is at least $|\langle n|n-1\rangle|^2p_{n-1}$. If $\tau\Delta << 1$, where $\Delta = (\langle 0|H^2|0\rangle - \langle 0|H|0\rangle^2)^{\frac{1}{2}}$ is the dispersion of H we have

$$|\langle n|n-1\rangle|^2 \approx 1 - (\tau\Delta)^2,\tag{73}$$

whence

$$1 \ge p_n \ge (1 - (\tau \Delta)^2)^n. \tag{74}$$

At a time T, when $n = T/\tau$ measurements have been made, the right side approaches $e^{-\tau T\Delta^2}$. Thus given any finite time T and dispersion Δ one can choose a sufficiently small interval τ between measurements that the initial state $|0\rangle$ is "coaxed" by the sequence of measurements into a mixed state so dominated by $|n\rangle$ that the entropy increase is arbitrarily small. (The so-called "watchdog" effect or "quantum Zeno effect" occurs when the repeated measurements are made in a frame containing the initial state which supresses the evolution altogether.)

Thus, while collapse due to measurement cannot be reproduced by unitary dynamics, a fact that gives rise to the measurement problem, we see that the converse is not true, i.e. unitary dynamics can be reproduced to arbitrary accuracy by a sequence of collapses. It is thus theoretically possible that what appears to us as Schrödinger evolution is a very good approximation to a process in which an interaction Hamiltonian "guides" a sequence of collapse processes happening during very small time intervals. By choosing τ small enough no increase in entropy would be detected even on a cosmic time scale.

10 Appendix

For conventient reference we here reproduce the derivation [13, 15] of the relationship between p and the d-metric in the conventional model and local hidden variable theories.

In a local hidden variable theory one has a set Λ with a measure μ such that

$$p(x,y) = \mu(\Lambda(x) \cap \Lambda(y)), \quad \mu(\Lambda(x)) = 1, \forall x.$$
 (75)

To evaluate the d-metric we must compute the supremum over z of. $|\mu(\Lambda(x) \cap \Lambda(z)) - \mu(\Lambda(y) \cap \Lambda(z))|$. But we note that the contribution coming from any overlap of $\Lambda(x)$ and $\Lambda(y)$ will cancel. Hence one can compute the z maximizing the expression as if the sets are disjoint. This occurs when either z = x or z = y and gives $1 - \mu(\Lambda(x) \cap \Lambda(y))$ whence

$$d(x,y) = 1 - p(x,y) (76)$$

which disagrees with (41).

In the CRQM we have (reverting to Dirac notation):

$$p(x,y) = |\langle x|y\rangle|^2 = Tr(\pi(x)\pi(y)), \quad \pi(z) \equiv |z\rangle\langle z|, \tag{77}$$

whence

$$d(x,y) = \sup_{z} |Tr(\pi(x)\pi(z)) - Tr(\pi(y)\pi(z))| = \sup_{z} |\langle z|\pi(x) - \pi(y)|z\rangle|.$$
 (78)

But this is just the largest eigenvalue of $\pi(x) - \pi(y)$. Since the π 's are projectors:

$$(\pi(x) - \pi(y))^3 = (1 - |\langle x|y\rangle|^2)(\pi(x) - \pi(y)) \tag{79}$$

and one reads off the largest eigenvalue to obtain (41).

Acknowledgements

I am gratefull to Prof. Philip Goyal and the Perimeter Institute for hosting the "Reconstructing Quantum Mechanics" conference in 2009 which led me to revisit my 1994 paper and resulted in significant simplifications in the argument. Conversations with Prof. Wm. Wootters at the conference led me to think further about the problem of eliminating exotic alternatives to conventional quantum mechanics which together with the paper of Stotland et al. stimulated the approach taken in this paper.

References

- [1] G.D. Birkhoff and J. von Neumann, Ann. Math. 37, 823 (1936).
- [2] A.M. Gleason, J. Math. & Mech. 6 885 (1957).
- [3] S. Sykora, Journal of Statistical Physics, Vol.11, No.1, pp 17-27 (1974)
- [4] W. Wootters, Foundations of Physics 20, 1365 (1990)
- [5] A. Stotland, A. Pomeransky, E. Bachmat, and D. Cohen Europhysics letters, Vol. 67, pp. 700–706, 2004, arXiv:quant-ph/0401021v2
- [8] B. Mielnik, Commun. Math. Phys. 15 1-46 (1969).
- [9] L. Hardy arXiv: "Quantum Theory From Five Reasonable Axionms" quant-ph/0101012v4
- [10] Christof Teuscher & Douglas Hofstadter (2004). "Alan Turing: Life and Legacy of a Great Thinker. Springer." p. 54. ISBN 3540200207.
- [11] J. von Neumann, "Mathematical Foundations of Quantum Mechanics", Princeton University Press, (1955) p. 365.
- [12] W. Sierpinski, "Introduction to General Topology", U. Toronto Press (1934).
- [13] D.I. Fivel, Phys. Rev. Lett. **67**, 285 (1991)
- [14] R.J. Bumcrot, "Modern Projective Geometry", Holt, Reinhart, Winston, Inc. p.23 (1969)
- [15] D. I. Fivel, Phys Rev A 50, No 1, 2108, (1994) arXiv:hep-th/9405042v1